*DOI:*
10.1093/ips/olx019

*Document Version*
Peer reviewed version

# Assembling (non)knowledge: Security, law, and surveillance in a digital world


## Abstract

Critical analyses of security have focused on the production of knowledge, techniques and devices that tame unknowns and render social problems actionable. Drawing on insights from Science and Technology Studies and the emerging interdisciplinary field of 'ignorance studies', this article proposes to explore the enactment of non-knowledge in security and legal assemblages. Starting with legal challenges brought against the NSA and other intelligence agencies after the Snowden revelations about mass surveillance, it shows how different modes of non-knowledge are enacted and not just 'tamed': uncertainty, ignorance, secrecy, ambiguity, and error. The enactment of non-knowledge has important implications for how we understand security practices, the relation between security and law, and public challenges to mass surveillance in a digital world. On the one hand, the enactment of non-knowledge by security and legal professionals limits activist and NGO resistance to mass surveillance, when these are focused on claims to knowledge, disclosure and transparency. On the other, reassembling non-knowledge and knowledge differently has generative political effects and opens new possibilities for intervention and resistance.


## Introduction

On 26 February 2013, a few months before the Snowden revelations, in a case filed by Amnesty International and a coalition of NGOs back in 2008 against the NSA collection of telephone metadata for intelligence purposes, the US Supreme Court decided that the plaintiffs did not have 'legal standing' to sue the US government (Clapper v Amnesty International USA 2013a). According to the majority opinion, the plaintiffs could not establish legal standing on an 'objectively reasonable likelihood standard', as they did not fulfil the criteria that 'threatened injury must be certainly impending to constitute injury in fact' (Clapper v Amnesty International USA 2013a, 2). Thus, the Supreme Court found that Amnesty's challenge that their communications could be intercepted by the NSA was based on a 'highly speculative fear' (Clapper v Amnesty International USA 2013a, 11). Drawing on previous judicial decisions, the US Supreme Court held that 'allegations of possible future injury' are not sufficient to ensure standing and the argument by Amnesty International and other international NGOs that their communications might be monitored by the NSA was based on a 'highly speculative chain of possibilities' (Clapper v Amnesty International USA 2013a, 18). The Court also stated, in a reinforced negative, that 'We *decline* to *abandon* our usual *reluctance* to endorse standing theories that rest on speculation about the decisions of independent actors' (Clapper v Amnesty International USA 2013a, 15 emphasis mine).

After the Snowden revelations in June 2013, mass surveillance in US has been

challenged in an increasing number of legal cases.[1] All these cases continued to debate questions of knowledge, speculation, likelihood and uncertainty. In the US, case after case was dismissed post-Snowden with similar justifications as the US Supreme Court had reached pre-Snowden: speculation and conjecture. In the most recent case brought again the NSA's upstream internet surveillance in 2015, the District Court of Maryland finds that the plaintiffs' allegations 'depend on suppositions and speculation, with no basis in fact, about how the NSA implements Upstream surveillance' (Wikimedia et al v NSA 2015b, 17). Even when legal standing is accepted, questions of likelihood, speculation and conjecture remain central (ACLU v Clapper 2013, 2015, Jewel v NSA 2015, Wikimedia et al v NSA 2015b).

At first sight, these statements resonate with the literature on law and anticipatory security as they appear to reinforce the distinction between law as relying on norms, generality and some understanding of linear temporality and future-oriented security as speculative and based on uncertainty (e.g. Scheuerman, 1994; Scheuerman, 2006a). Yet, rather than preemptive security practices undoing legal provisions and fundamental rights, it is the rights claims by activists and NGOs that are deemed to rely on speculation and conjecture. Courts also continued to reiterate their basis in factuality against uncertainty and the NGOs' conjectures both before and after the Snowden revelations. What do these developments post-Snowden mean for the relation between security, law and knowledge in a digital world?

This article argues that a key stake in challenges to mass surveillance has been the enactment of non-knowledge. Courts, security professionals and activists made claims not only about the validity and legitimacy of knowledge (Gros, de Goede, and İşleyen 2017), but also about what counts as non-knowledge. I show how NSA representatives and the US government often do not argue from the position of knowledge, but exactly from that of non-knowledge. In these controversies, non-knowledge is enacted as uncertainty, ignorance, secrecy, ambiguity and error, assembled and reassembled to reconfigure attributions and subjects of knowledge and non-knowledge.

Drawing on recent debates on non-knowledge and ignorance in sociology and Science and Technology Studies (STS) and the emerging field of 'ignorance studies', I propose to supplement analyses of knowledge controversies (Whatmore 2009) and 'epistemic practices' (Bueger 2015) with practices of and controversies over non-knowledge. The article is also an invitation to critical approaches to security and international political sociology (IPS) to engage with the growing literature on agnotology in STS and ignorance studies. Rather than advancing an exhaustive taxonomy of non-knowledge, it explores how specific modes of non-knowledge have emerged in the controversies over mass surveillance. Reconfiguring these controversies in terms of assembling knowledge and non-knowledge has important political implications for academic and public interventions against mass surveillance in a digital world.

My argument will proceed in three stages. The first outlines the main debates around non-knowledge and ignorance in order to develop an agnotological approach to legal and

[1] The most prominent US legal cases against NSA surveillance have been *Klayman v Obama* (I and II), *Jewel v NSA, ACLU v Clapper, First Unitarian Church v NSA, Smith v NSA, Schubert v NSA* and, most recently, *Wikimedia v NSA*. A series of legal challenges have been mounted in Europe as well: the most notable decisions have been by the European Court of Justice in *Schrems v Facebook* and by the European Court of Human Rights in *Zakharov v Russia*. ECHR decisions in legal challenges concerning GCHQ surveillance are still pending (*Big Brother Watch and Others v The United Kingdom, 10 Human Rights Organisations and Others v The United Kingdom*). Given limits of space, the US legal challenges are the key focus of this paper.

security assemblages. The second section explores the enactment of non-knowledge in a series of legal cases contesting mass surveillance. A third section shows how knowledge and non-knowledge are assembled and reassembled in ways that challenge existing attributions of what counts as 'the other side of knowledge', thus opening possibilities for intervention and resistance. A novel understanding of resistance to mass surveillance emerges: one that does not exclusively challenge dominant knowledge, but contests the attribution, practices and subjects of non-knowledge. In conclusion, I develop a series of implications that the agnotological approach proposed here entails for IPS and political controversies over mass surveillance in a digital world.

## Enacting non-knowledge: from epistemology to agnotology

Taming unknowns has been key to critical discussions of security, risk and uncertainty in security studies and IPS. In attending to the specificities of law-making processes, governmental techniques, expert practices and the production of preemptive and anticipatory security knowledge (Adey, Anderson, and Graham 2015, Amoore 2014, Anderson 2010, Aradau and van Munster 2011, de Goede 2012, de Goede and de Graaf 2013, Neal 2012, Opitz and Tellmann 2015), critical scholars have shown how the orientation to the future challenges established modes of legal reasoning. Future-oriented security practices insert radical uncertainty at the heart of legal reasoning (Amoore 2008, de Goede and de Graaf 2013, Kessler 2011) and thus highlight key tensions between security and legal knowledge production. Radical uncertainty challenges both the aspect of defuturisation – law as creating continuity of expectations – and law's orientation towards the past by inviting law 'to speculate on deeds not yet committed' (Opitz and Tellmann 2015, 17). Understood as an epistemic practice, law is constantly articulated with different modes of knowledge, making it particularly susceptible to security matters (Krasmann 2012, 381). Louise Amoore has also argued that exceptional measures such as preventive detention or biometrics 'operate in place of, and in advance of the legal thresholds of evidence and decision' (Amoore 2008, 847).

Digital technologies have only intensified these tensions between security and law, as the future orientation of digital data – devoid from attention to real people and places – sets these practices in stark contrast with the past orientation of law. The 'ontology of association' characteristic of the security derivative is firmly placed in the realm of imagination and breaking away from the past-orientation of legal evidence (Amoore 2011, 2). Similarly, transactional data turns knowledge about past behaviour into a 'form of actionable intelligence', which enables 'the *preemption* of what could be terrorist schemes or attacks' (Amoore and de Goede 2008, 178 italics in original). These analyses of anticipatory knowledge have shed light on the fragility of legal knowledge, which is increasingly 'undone' by digital technologies and future-oriented security practices.

Understanding law and security as practices of knowledge production has focused critical debates on the contestation, translation and potentially 'colonization' of law by other forms of knowledge (Valverde 2003, 15). I propose to supplement these analyses by exploring non-knowledge in legal and security assemblages, or what I call – following Robert Proctor's coinage – an agnotological approach. As this section shows, an agnotological approach attends

to how security practices do not just tame but also enact unknowns. Moreover, enacting non-knowledge is neither limited to uncertainty, nor singular to security professionals. The next section will develop a close reading of legal cases challenging mass surveillance to show how law and security are enacting and assembling knowledge and non-knowledge.

Over the past decade, there has been a growing interest in ignorance and non-knowledge in Sociology, Science and Technology Studies (STS) and the emerging field of 'ignorance studies' (Gross and McGoey 2015). Despite productive intersections between STS, critical approaches to security and IPS, these have not extended to the body of work on agnotology. Ulrich Beck's own vocabulary of non-knowledge has gone unnoticed until very recently in favour of his theorisation of 'risk society' (for an exception see Kessler 2010, Gross 2016). This is possibly due to the fact that Beck turned to non-knowledge relatively late in his career (Gross 2016) and that non-knowledge is a rare usage in English. Although the Oxford English Dictionary (2003) traces the use of non-knowledge to the Rolls of Parliament in 1503, the word has not gained wide circulation in comparison with ignorance. The study of non-knowledge also appears, to some extent, counterintuitive and explains the preference for the terminology of ignorance. For Beck (2009, 123), non-knowledge can be 'conscious or unconscious, concrete or theoretical, it can signify wilful ignorance or an inability-to-know'. It is, however, the inability-to-know or the 'unknown unknowns' that have become mostly associated with non-knowledge in Beck's work and subsequent debates, echoing Rumsfeld's (in)famous matrix. For instance, Gross argues that 'non-knowledge or ignorance can be referred to as a realm that escapes recognition' (Gross 2010, 60, see also Daase and Kessler 2007). In security studies, Rumsfeld's matrix of non-knowledge has been mostly used to render the forms that international dangers and risks can take (Rasmussen 2006, Daase and Kessler 2007, Aradau and van Munster 2011). Thus, there has been less attention to how non-knowledge is enacted in the practices of security governance.

The STS literature has focused exactly on the enactment of ignorance and non-knowledge in scientific knowledge practices. Proctor's coinage of 'agnotology' aimed to capture the study of 'the conscious, unconscious, and structural production of ignorance, its diverse causes and conformations, whether brought about by neglect, forgetfulness, myopia, extinction, secrecy, or suppression' (Proctor 2008, 3). Rather than representing ignorance as the absence of knowledge or the 'unknown unknowns' of a complex and unpredictable world, agnotology approaches ignorance as socially constructed, positive and generative of political effects. Agnotological studies have explored the mobilisation and deployment of ignorance within public controversies about scientific knowledge, from Proctor's (2011) work on the tobacco industry, Oreskes and Conway's (2011) analysis of the production of 'doubt' about climate change science and Mirowski's (2013) diagnosis of the failure of critiques of neoliberalism. For instance, Mirowski has argued that 'the deployment of agnotology is a major hallmark of the neoliberal thought collective', and that it has been a key strategy for unmaking calls for reform in the wake of the 2008 financial crisis by 'filling the public sphere with fog' (2013: 442). Similarly, Oreskes and Conway trace the production of doubt through the creation of public controversies that 'take uncertainties out of context and leave the impression that *everything* is unresolved' (2011: 53 italics in original). However, the literature on agnotology has often tended to emphasise individual actors and networks of state-academic-market actors. Mirowski and Nik-Khah clarify the remit of agnotology as the 'focused study of the intentional

manufacture of doubt and uncertainty in the general populace for specific political motives' (2013, 281) rather than the more general study of socially constructed ignorance. Thus, many of the empirical studies have focused mostly on the systemic and deliberate manufacture of ignorance (Pinto 2015: 295).

Feminist work on 'epistemologies of ignorance' has moved beyond the realm of scientific knowledge production and the intersection between business and science to understand how variegated practices of power/ignorance limit the capacity of groups and individuals to exercise political agency. Nancy Tuana has enjoined feminist scholars to 'understand the practices that account for not knowing, that is, for our *lack* of knowledge about a phenomenon or, in some cases, an account of the practices that resulted in a group *unlearning* what was once a realm of knowledge' (2004: 195 italics in original). Similarly to the agnotological approach proposed by Proctor, epistemologies of ignorance see ignorance as positive, a social enactment and not 'mere absence of knowledge, not as a void but as a force all its own which often blocks knowledge, stands in its place, and tacitly or more explicitly affirms a need or a commitment not to know' (Code 2014, 154). The power of ignorance is entwined with the production of credible and incredible knowers, as well as with the reproduction of relations of (epistemic) domination. Mobilising Charles Mills' (1997) analysis of 'white ignorance', feminist scholars have shown how a racial and gendered 'contract of ignorance' both insulates the dominant from the knowledge about the world they have created, and reproduces epistemic injustice and epistemically disadvantaged subjects.

More recently, the emerging interdisciplinary field of 'ignorance studies' has proposed to bring together these different approaches in order to theorise ignorance as 'a regular feature of decision-making in general, in social interactions and in everyday communication' (Gross and McGoey 2015, 23). Thus, ignorance rather than non-knowledge has become the overarching term for broader, interdisciplinary agnotological analyses. The terminology of ignorance is problematic to some extent as it carries negative assumptions; Beck and his students prefer to use the coinage of *Nichtwissen* in German (usually translated as 'non-knowledge' in English). Even as ignorance is understood as a 'stratified object with multiple levels and layers' (Caduff 2015, 38), agnotology has paid less attention to how ignorance is differentiated and contested in relation with other modes of non-knowledge. Mirowski's (2013) use of ignorance in the neoliberalism debates becomes largely equivalent to uncertainty or fog. In Oreskes and Conway's (2011) work on climate change, the production of doubt is equated with confusion, ignorance and uncertainty. Even when scholars have proposed taxonomies of ignorance, which attend to differences between risk, uncertainty, vagueness, ambiguity, error and so, these taxonomies have been limited (Gross 2010, Smithson 2008). I argue that the very use of 'ignorance' as an overarching term risks limiting attention to how different modes of non-knowledge are enacted and how controversies emerge over what counts as knowledge and non-knowledge. It is perhaps telling that Rumsfeld's matrix of known knowns, unknown unknowns and unknown knowns obscures considerations of secrecy or error in security practices.

The agnotological approach I propose here takes the enactment of and controversies over different modes of non-knowledge as its starting analytical point. In similar ways in which STS have suggested that science generates non-knowledge, I analyse law and security as assemblages generative of non-knowledge and controversies over what counts as knowledge

and non-knowledge.[2] Or, as Beck and Wehling ask in a recent text, 'How is non-knowing becoming a topic of political controversies and a political resource, and what different dynamics of a politics of non-knowing may be observed?' (2012, 51).[3] I do not aim to develop an exhaustive taxonomy or definition of non-knowledge, but to explore how non-knowledge is enacted, how heterogeneous modes of non-knowledge become the object of controversies, and have political effects. The vocabularies of non-knowledge mobilised in public controversies – from risk and uncertainty to ambiguity, error, surprise, complexity, confusion, omission, fallacy or contingency – are more complex and varied than existing taxonomies have captured so far. Exploring the 'dynamic connections' (Gross 2007) between modes of non-knowledge and the assembling of knowledge and non-knowledge can offer renewed resources for critique and political intervention. The next section turns to the enactment of non-knowledge in legal cases brought by NGOs and activists before US courts in the wake of the Snowden revelations. How do security professionals, legal professionals, NGOs and other experts enact different modes of non-knowledge, how do they contest attributions of knowledge and non-knowledge, and with what effects for political action?

**'In the twilight of probability': non-knowledge between law and security**

In December 2013, just a few months after the Snowden revelations and after the US Supreme Court dismissed the Amnesty International case against the US government, Judge Pauley III dismisses the first post-Snowden case filed by the American Civil Liberties Union in June 2013 (ACLU v Clapper 2013). Although the judge acknowledges that the plaintiffs have acquired knowledge about NSA metadata surveillance through the Snowden revelations, his decision highlights the persistent problem of non-knowledge:

> Fear that telephony metadata relating to the ACLU will be queried or reviewed or further investigated 'relies on a highly attenuated chain of possibilities.' Amnesty Int'l, 133 S. Ct. at 1148. '[S]uch a fear is insufficient to create standing,' Amnesty Int'l, 133 S. Ct. at 1152. Neither can it establish a violation of an individual's First Amendment rights. (ACLU v Clapper 2013, 47)

Judge Pauley's reasoning relies on the US Supreme Court decision in *Clapper v Amnesty International*, preceding the Snowden revelations, that the plaintiffs could 'present no concrete evidence to substantiate their fears, but instead rest on mere conjecture about possible governmental actions' (Clapper v Amnesty International USA 2013a, 21). Conjecture delegitimises the NGOs' constitutional claims before the law. This reasoning is repeated across courts in the US and it concerns both metadata collection and 'upstream' surveillance through data capture at internet 'backbone' networks. In the most recent US case against mass

[2] I use assemblage here in Paul Rabinow's sense of an 'experimental matrix of heterogeneous elements, techniques and concepts' (2003, 56).

[3] In his later work on world risk society, Ulrich Beck problematizes the concept of non-knowledge. Particularly in the collaborative work with Wehling, non-knowledge becomes central as they see the 'co-production of knowledge and non-knowledge' as central to our societies (Beck and Wehling 2012, 45). The move to non-knowledge is very different from Beck's earlier statements about politicians who do not know but feign knowledge.

surveillance, the US government has argued that the plaintiffs' arguments are 'remarkably similar' to the ones in *Amnesty International* (Wikimedia et al v NSA 2015a, 44).

Yet, the earlier decision in *Clapper v Amnesty International* has an interesting split (5-4) and a dissenting opinion, written by Justice Breyer, which is underpinned by a different understanding of law's knowledge and non-knowledge. While the 5-4 split has often been read along ideological lines of republican versus democrat, Sheila Jasanoff's analysis of divergences between Justice Scalia and Justice Breyer in US Supreme Court decisions shows that Breyer's decisions draw on 'expert accounts of reality', while Scalia sees the law as the 'unambiguous baseline on which reason is built; the law prescribes who can speak, who can challenge, and, in contested cases, whose reason prevails' (Jasanoff 2011, 330). Given Breyer's view of the relation between law and expert knowledge and his long-standing interest in risk regulation and uncertainty, his dissent in *Clapper v Amnesty International* can be read as a different understanding of the relation between law and (non)knowledge. For Breyer, law is entwined with uncertainty and it is mobilised in the 'game' of knowing and not-knowing. Breyer thus holds that the likelihood of the plaintiffs having their communications intercepted in the future is not speculative, but a reasonable inference:

> The future is inherently uncertain. Yet federal courts frequently entertain actions for injunctions and for declaratory relief aimed at *preventing future activities that are reasonably likely or highly likely, but not absolutely certain*, to take place. And that degree of certainty is all that is needed to support standing here (Clapper v Amnesty International USA 2013b, 10 Breyer, J, dissenting, my italics).

Drawing on an analogy with everyday reasoning about risk and likelihood, Breyer presents an understanding of law as being able to address future events:

> One can, of course, always imagine some special circumstance that negates a virtual likelihood, no matter how strong. But the same is true about most, if not all, ordinary inferences about future events. Perhaps, despite pouring rain, the streets will remain dry (due to the presence of a special chemical). But ordinarily a party that seeks to defeat a strong natural inference must bear the burden of showing that some such special circumstance exists. […] Consequently, we need only assume that the Government is doing its job (to find out about, and combat, terrorism) in order to conclude that there is a high probability that the Government will intercept at least some electronic communication to which at least some of the plaintiffs are parties.[4] (Clapper v Amnesty International USA 2013b, 10 Breyer, J, dissenting)

Justice Breyer's reference to a 'degree of certainty' echoes the understanding of uncertainty in law going back to the seventeenth century. Uncertainty and certainty are not mutually exclusive in legal reasoning, but are intimately entwined through probabilistic reasoning. As Ian Hacking (Hacking 1975, 86) reminds us, '[p]robability is not new to law'. Yet, it is not mathematical probability, usually associated with statistical risk techniques in the IR literature, that has been

[4] Breyer is the author of several books and articles on risk and regulation (e.g. Breyer 1993).

central to legal reasoning, but epistemic probability. Ian Hacking has succinctly summarised this dual nature of probability: statistical probability is concerned with 'stochastic laws of chance processes', while epistemological probability gauges 'reasonable degrees of belief in propositions quite devoid of statistical background' (1975, 12). It is probability in this latter sense of 'degrees of certainty' that has long shaped legal reasoning, evidence and proof.

Courts make decisions based on less than certain evidence. However, these decisions have to be produced as reasonable. As Barbara Shapiro's seminal work on the history of law and probability has shown, the emergence of ideas of moral certainty, degrees of certainty, and the reasonable man were integral to the shift from 'the traditional philosophical norm of the demonstrably certain toward a more probabilistic view of human knowledge and natural science' (Shapiro 1983, 15). She draws on John Locke's reading of epistemic probabilities as key to law and decisions on evidence to show that, in the absence of certainty, judgements were made on the basis of probability. For Locke, the degrees of certainty in our knowledge span a continuum 'from the very neighbourhood of certainty and demonstration, quite down to improbability and unlikeness, even to the confines of impossibility; and also degrees of assent from full assurance and confidence, quite down to conjecture, doubt, and distrust' (Locke 2004 [1689], 800). Conjecture was at the lower end of Locke's continuum of probabilities, not far from ignorance, but it was also deemed able to be transformed into probabilistic judgement. Therefore, invocations of conjecture and speculation need to be situated within these debates that did not oppose certainty and uncertainty, but aimed to draw a line between different modes of acceptable and unacceptable uncertainty.

Thus, law meshes certainty and uncertainty through the calibration of epistemic probabilities. Even when mathematical or statistical probability came to demarcate natural science from law, for instance, epistemic probabilities have continued to shape legal reasoning, which 'has been modified since [Locke] only in particulars' (Shapiro 1983, 193). The use of different standards of reasonableness means that law reasons 'in the twilight of probability' (Locke 2004 [1689]).[5] When courts dismiss the NGOs' claims as conjecture, they effectively rely on a long history of legal reasoning where conjecture is at the lower end of Locke's continuum of uncertainty. Nonetheless, this history of legal reasoning is simultaneously rendered unknown, as discourses of scientific method have instituted a strong distinction between factual certainty and conjectural or speculative uncertainty in legal reasoning.[6]

Ultimately, I suggest reading these cases as controversies over non-knowledge and not just knowledge. Conjecture and speculation name unacceptable degrees of uncertainty and are therefore relegated to the realm of non-knowledge. In the latest response to the decision to dismiss the *Wikimedia et al v NSA* case, the plaintiffs argue that their arguments are represented as relying on probabilities and therefore speculation, thus undermining the acceptability of 'deduction, reasonable inference, and expert opinion' in legal cases to establish knowledge claims (Wikimedia et al v NSA 2016). However, by asserting a strong distinction between certain facts and uncertain probabilities, the plaintiffs inadvertently adopt a similar position to that of Justice Scalia and Judge Pauley in previous cases.

[5] Compare the interpretation of reasonable as the ordinary 'man on the Clapham omnibus' by Didier Bigo and Elspeth Guild (2007).

[6] Even as scientists have started to challenge this strong distinction, it is operative in many social fields.

This distinction is also adopted by security professionals, thus reinforcing the relegation of NGOs' claims to a zone of non-knowledge. For instance, in a testimony before the court in *ACLU v Clapper*, James Clapper, former Director of National Intelligence, invokes the earlier Supreme Court decision to argue that the plaintiffs still do not have standing as they cannot show 'injury in fact':

> The Supreme Court has made clear, however, that the mere fact that the government may have obtained information associated with plaintiffs' telephone calls does not demonstrate standing where, as here, plaintiff' allegations are premised on a theory of 'subjective chill' arising from a speculative fear that the government might 'in the future take some other and additional action detrimental to them with that information' (Clapper et al. 2014, 24).

The opposition of factuality and certainty on the one hand and speculation and uncertainty on the other is only possible to the extent that the probabilistic language of law – 'probable cause' or even 'reasonable suspicion' – is recast in the language of scientific method.

Yet, the assembling of fact and certainty on one side against uncertainty and probability on the other does not mean that all uncertainty is ascribed to a zone of non-knowledge. The vocabulary of likelihood and reasonableness is deployed by security professionals to characterise their own knowledge production when they point out that, for instance, the 'NSA may target under this certification [section 702 of the Foreign Intelligence Surveillance Act] non-United States persons reasonably believed to be located outside the United States who possess, are expected to receive, and/or are likely to communicate foreign intelligence information' (Ledgett 2007, 3). Here, security professionals sever reasonableness and factuality by adopting a probabilistic language of legal standards, which calibrates uncertainty and certainty but does not see them as mutually exclusive. The language of probabilities and reasonableness allows security professionals to manage uncertainty and calibrate the 'degrees of certainty' in their own production of knowledge. Thus, when NSA analysts are required to show that they have 'reasonable articulable suspicion' before querying a database, the legal standard is operationalised as low probability rather than high probability.[7] The differential enactment of uncertainty across legal and security practices remains, however, unquestioned.

Even conjectures and speculations become acceptable when they emerge in the process of producing security knowledge. In *ACLU v Clapper*, the NGOs' 'speculative' claims are deemed unacceptable, while the NSA's ability to produce speculative knowledge appears credible. The 'highly attenuated chain of possibilities' that Judge Pauley dismissed in the ACLU argumentation is deemed indubitable when deployed by the NSA:

> *No doubt*, the bulk telephony metadata collection program vacuums up information about virtually every telephone call to, from, or within the United States. That is by design, as it allows the NSA to detect *relationships so attenuated and ephemeral* they would otherwise escape notice. (ACLU v Clapper 2013, 52 my italics)

[7] For one of the most detailed discussion of the 'reasonable' standards used by the NSA as part of the so-called 'minimization' procedures, see the report by the Privacy and Civil Liberties Oversight Board (2014b).

NSA's 'attenuated and ephemeral relations' become ascriptions of knowledge in contrast to the 'highly attenuated chain of possibilities' that the plaintiffs allegedly mesh in a zone of non-knowledge. The contention that metadata can reveal potential terrorists in the future is not evaluated by the same standards as the NGOs' claims. By virtue of being speculative, the processing of metadata appears as 'eminently reasonable':

> It is eminently reasonable to believe that Section 215 bulk telephony metadata is relevant to counter-terrorism investigations. The government queries the telephony metadata to identify connections between suspected-terrorist selectors and their unknown contacts. JA 272. Bulk collection of telephony metadata makes it possible to draw those historical connections because there is no way to know in advance which metadata will be responsive to queries for those in contact with suspected-terrorist selectors (Clapper et al 2014: 32).

Conjectures are justified in the NSA actions, while being disqualified in the plaintiffs' claims. For the security professionals, conjecture is cast as the beginning of a journey towards knowledge, a mode of reducible uncertainty; for the NGOs, conjecture is the end of the road, an unsurpassable limit of irreducible uncertainty. This dual enactment of conjecture as reducible and irreducible uncertainty is made possible through the temporalisation of knowledge production as a process moving from uncertainty and conjecture to certainty and facts. The NSA's conjectures about 'what might be connected' appear both necessary and reducible in the process of knowledge generation, while the NGOs' conjectures remain irreducible. Given the dominance of the imaginaries of scientific method, this rendering of knowledge production is not challenged by NGOs. Rather, they attempt to establish their claims as factual and certain. This is in stark contrast to the security professionals, who do not only claim conjecture as reducible knowledge, but also make claims to non-knowledge, showing that non-knowledge and knowledge are not mutually exclusive. On the one hand, the NSA argues that metadata is supposed to connect 'fragmented and fleeting communications' on the path to know; on the other, the NSA also claims non-knowledge as it only collects information up to three hops and does not know the identity of the phone subscribers (ACLU v Clapper 2013, 52, 41). Security professionals simultaneously mobilise the language of knowledge and non-knowledge and thus limit challenges against mass surveillance.

This discussion of the differential enactment of conjecture and speculation shows how difficult it has been to challenge practices of mass surveillance, even when different spaces of political controversy have been opened (see also Gros, de Goede, and İşleyen 2017). Breyer has formulated one such challenge, which nonetheless failed to capture the entanglement of uncertainty and certainty through probabilistic reasoning. While this is partly due to the dominance of imaginaries about the scientific method in law and security, the next section will show how non-knowledge has also been reassembled in challenges against mass surveillance.

**Reassembling non-knowledge in public controversies**

If the deployment of uncertainty in legal and security reasoning has largely limited anti-surveillance actions, other modes of non-knowledge have made possible practices of reassembling that have challenged mass surveillance: secrecy, ignorance, ambiguity and error. In the fragile assemblage of knowledge and non-knowledge, secrecy, ignorance, ambiguity and error could be assembled differently. This section does not aim to offer an exhaustive analysis of the modes of non-knowledge enacted in the controversies over mass surveillance. For reasons of space, it will offer a set of illustrations of how reassembling non-knowledge has made possible political contestations of surveillance.

The arguments about speculation and conjecture discussed in the previous section have been entangled with questions of secrecy and ignorance. The 'state secrecy' argument has been pursued by the US government in legal cases concerning bulk data collection before the Snowden revelations. When the argument of state secrecy was challenged after the Snowden revelations, the US government engaged in a process of complex classification and declassification of documents. In so doing, it rearticulated secrecy through practices of limited declassification, thus demarcating areas of access and knowledge from zones of non-knowledge. As Brian Balmer (2006: 696) has argued, secrecy 'fractures and disrupts the topography of knowledge – providing particular geographically restricted accounts of the world'. Secrecy creates a spatial-epistemic regime, which separates spaces of knowledge and knowers from spaces of non-knowledge. The secret as boundary drawing does not just enact the status of those in the secret as credible knowers and producers of knowledge – it also delegitimizes the credibility of those who are not part of the community of secrets. As a tool of 'group formation', of 'control and the establishment of hierarchies' (Vermeir and Margocsy 2012: 162), secrecy enacts the boundary between knowing and not-knowing as inside/outside.

Therefore, what is at stake in the production of secrecy is not simply the removal of knowledge, the creation of 'blacked-out' spaces, or the drawing of boundaries through the multiplication of categories of classified documents, but equally the crediting or discrediting of subjects of knowledge. When articulated in relation to secrecy, the differentiation of reducible and irreducible uncertainty becomes starker, as NGOs and civil rights activists lack access to the laboratories of security. As Judge T.S. Ellis puts it in *Wikimedia v NSA* (2015b, 27), 'in a case like this, plaintiffs necessarily rely on probabilities and speculation because most facts about Upstream surveillance remain classified, and hence plaintiffs see through a glass darkly'. Here, secrecy, ignorance and uncertainty are mobilised in conjunction, so that the lack of access to the laboratories of security becomes read as ignorance inevitably leading to speculation and conjecture. At first sight, the assembling of secrecy and conjecture re-enacts the boundary between those who know and those who do not and deactivates anti-surveillance claims. Through the legal challenges mounted in various US courts, NSA representatives, experts and government lawyers have repeatedly argued from the position of non-knowledge. They have shifted attention from what has become publicly known about mass surveillance to the limits of public knowledge, to what we ignore about the specific operations of the programmes given the continued secrecy of classified information (e.g. Wikimedia et al v NSA 2015a).

Yet, secrecy, uncertainty and ignorance can also be assembled differently, as the US Court of Appeals for the Second Circuit did in *ACLU v Clapper* on 7 May 2015, under a month before the Patriot Act was due to expire. The Court reassembled non-knowledge to invalidate

the Congress support for Section 215 of the Patriot Act by arguing that 'Congress cannot reasonably be said to have ratified a program of which many members of Congress – and all members of the public – were not aware' (ACLU v Clapper 2015). Only a limited number of members of Congress had an understanding of the telephone metadata programme and most did not know whether the FISC interpretation of Section 215 of the Patriot Act was correct. The Court inserts a new subject of non-knowledge in the debate – neither security professionals, nor NGOs, but members of Congress. In so doing, the Court enacts members of Congress as ignorant due to the unjustified use of accelerated procedures and secrecy. The telephone metadata programme was 'shrouded in the secrecy applicable to classified information' (ACLU v Clapper 2015, 81). Given the secrecy around the provisions of the Patriot Act and ignorance of members of Congress about what metadata collection entailed, their assent to the bulk metadata programme is suspended as their knowledge is revealed as non-knowledge.

By enacting ignorance and new subjects of non-knowledge – members of Congress – the Court reassembles knowledge and non-knowledge in ways that avoid direct challenges either to secrecy or to the definition of legal standing. It does not broach the question of 'state secrets', which the US Government had initially raised to stop a range of cases from litigation. The state secret privilege had already been partially suspended in other NSA surveillance litigation 'given the multiple public disclosures of information regarding the surveillance program' (Jewel v NSA 2013). At the same time, judges have also accepted that the state secrets privilege 'would apply to bar disclosure of significant materials related to the alleged Program' (Jewel v NSA 2013). In ACLU v Clapper (2015), the Court also continues the practice of previous judgements of not challenging the assumptions of conjecture and speculation as it defers to Congress to discuss the 'reasonableness' of the Government's assertions as to what data is needed for national security. However, by introducing a new mode of non-knowledge, it destabilises the existing assemblage. Here, the Court enacts a tactic similar to Jacques Rancière's (1991) ignorant schoolmaster, Joseph Jacotot: Jacotot overturns the relation between the master supposed to know and the supposedly ignorant students by teaching what he does not know. Similarly, the Court inverts the logic of security professionals supposed to know and the NGOs' irreducible uncertainty not by claiming better or more valid knowledge but by inserting a different mode and subject of non-knowledge: the ignorance of members of Congress.

Alongside ignorance and secrecy, ambiguity has also been deployed both to foster non-knowledge and to (de)stabilise the assembling of ignorance, uncertainty and secrecy. Ambiguity has been often invoked in conjunction with uncertainty to justify the intelligence agencies' secrecy: 'to create in the minds of potential malefactors significant ambiguity and uncertainty about which channels of communication might be safe and which channels of communication are likely to be monitored' (Home Affairs Committee 2014, Ev 61 by Nigel Inskter). In the oral hearing in another anti-surveillance case in the US, *Jewel v NSA*, Richard Wiebe notes for the plaintiffs that 'we have confronted in this case shifting uses of terms like "acquiring", "collection", "capturing", and that's why we have had divided things into stages' (Jewel v NSA 2014, 54). The production of ambiguity about NSA practices is effectively a form of non-knowledge that affects not only malevolent others, but anti-surveillance activists and NGOs.

Jacqueline Best has distinguished ambiguity from uncertainty, as the former 'emphasizes the central role played by interpretation and its effects on our efforts to communicate and act' (Best 2012, 677) and it is fostered as a resource for governing (Best 2009, 2012). While ambiguity in this sense would be intrinsic to legal interpretation and public controversies, ambiguity as enacted by the NSA's use of terminology produces 'fog' about surveillance practices and relegates NGOs and activists to a zone of non-knowledge. As mentioned earlier, the intelligence agencies have placed particular emphasis on use the language of 'intelligence collection' or 'bulk metadata collection' (Clapper 2013) to avoid public criticism of mass surveillance. The ambiguity of 'collection' allows both for the inclusion of a range of processes – encompassing data analytics – and the refutation of the criticism of mass surveillance. In criticising the NGO and activist references to the practices of 'mass surveillance', security professionals in the UK have coined the ambiguous terminology of 'bulk powers' (Anderson Q.C. 2016). 'Bulk' is etymologically associated with commodities rather than people and thus eschews connotations of surveillance by humans, drawing on an implicit differentiation of data processing by humans and by computers, often invoked in the justification of intelligence agencies' practices (see Aradau and Blanke 2015).

In its report on the NSA telephone metadata programme, the Privacy and Civil Liberties Oversight Board (PCLOB) also notes how ambiguity about the practices of data collection is enacted:

> While the NSA's upstream collection is intended to acquire Internet *communications*, it does so through the acquisition of Internet *transactions.* The difference between *communications* and *transactions* is a significant one, and the government's failure to initially distinguish and account for this distinction caused the FISA court to misunderstand the nature of the collection or over two years… (Privacy and Civil Liberties Oversight Board 2014, 39 italics in original)

The ambiguity of 'communication'/'transaction' underpinned the NSA claim that it conducted targeted surveillance of foreigners outside the US, who were a legitimate foreign intelligence interest. This ambiguity sustained non-knowledge about the inevitable collection of relational or transactional data, therefore data that entails more than the target of surveillance.

Challenging ambiguity, however, cannot be reduced to a call for clarity or precision, as ambiguity is intrinsic not only to legal reasoning but to language more generally. The question that the PCLOB raises is that the use of ambiguity obfuscates NSA practices and enacts non-knowledge for subjects in charge of oversight and therefore supposed to know. The PCLOB destabilises the assembling of ambiguity, secrecy and ignorance by redrawing the lines between subjects of knowledge and subjects of non-knowledge. The ACLU has similarly argued that the government has used the ambiguity between 'collection of data' and 'reviewing data' to dismiss the NGOs' claims as 'speculative prospect' and base their standing upon the collection of data as seizure (ACLU v Clapper 2015). However, the ACLU's general claims about ambiguity at the expense of relations with other modes of non-knowledge have failed to destabilise the assemblage of non-knowledge in similar ways as the PCLOB has done.

Finally, the legal challenges have perhaps unsurprisingly also raised the problem of error. Court judgments are held to have been made in error (Jewel v NSA 2014, Wikimedia et

al v NSA 2016). At times, some errors are deemed preferable over others, as the error of 'closing the courthouse doors to a plaintiff who suffers an actual injury' is rendered less important than the error of proceeding with litigation that challenges the powers of other branches of government (Wikimedia et al v NSA 2015b, 27). This distribution of errors turns upside down the distinction between the most serious judicial error of convicting an innocent person and the less serious judicial error of not convicting a guilty one. Relations between branches of government are elevated above the constitutional rights of citizens. Errors are also the result of non-knowledge in a digital world – unlike the NSA experts, NGOs are deemed to make errors in their claims given their lack of knowledge about the Internet and NSA programmes. However, when the NSA's own errors are brought into public view, error also destabilises ascriptions of non-knowledge and demarcations between more or less acceptable errors. The Privacy and Civil Liberties Oversight Board raised the production of error as a central element of oversight and reporting for the NSA (Privacy and Civil Liberties Oversight Board 2014). Introducing oversight over the production of errors in NSA's data collection, review and reporting, the PCLOB also reconfigures the zones of knowledge and non-knowledge.

The agnotological analysis developed here has shown that enacting non-knowledge and (re)assembling uncertainty, ignorance, secrecy, uncertainty, ambiguity or error become key stakes in these public controversies over mass surveillance. Moreover, it is the reassembling of non-knowledge that opens new possibilities for contesting mass surveillance. Even though reassembling non-knowledge has opened new possibilities for resistance, so far NGOs and anti-surveillance activists have only marginally mobilised non-knowledge and have continued to largely focus on the production of knowledge about NSA surveillance, practices of data collection and data analytics. I suggest that resistance to surveillance practices needs to intervene through reassembling non-knowledge, however counterintuitive such a political move might appear at first sight.

## Conclusion

Critical research in security studies and IPS has offered detailed analyses of heterogeneous assemblages that are deployed in governing insecurity and risk. They have highlighted regimes of power/knowledge, networks of expertise and discursive-material entanglements. Drawing on STS and the emerging interdisciplinary field of 'ignorance studies', this article has proposed to supplement analyses of knowledge assemblages and epistemic practices with practices of and controversies over the enactment of non-knowledge. Although a rich literature has emerged at the intersection of STS and IPS, there has been scant attention to the growing body of work on agnotology.

The analysis developed here is an invitation to IPS and critical approaches to security to attend to the enactment of non-knowledge and not just knowledge, to supplement regimes of power/knowledge with power/non-knowledge, and knowledge controversies with non-knowledge controversies. While contributions to IPS have highlighted the 'blindspots' of ambiguity (Best 2009) and secrecy (Walters and Luscombe 2017), I have argued that we need to explore heterogeneous modes of non-knowledge, their entanglements and (re)assembling.

Rather than an exhaustive taxonomy of non-knowledge, the agnotological approach I have proposed here develops an analysis of non-knowledge as enacted and (re)assembled in public controversies. It thus asks for closer attention to the heterogeneity of non-knowledge and its political deployment, without subsuming it to a strategic use of ignorance as the literature on agnotology has tended to do.

In taking a series of legal cases as sites of encounter between security professionals, judges, lawyers and anti-surveillance activists, I have shown how non-knowledge becomes a key political stake in public controversies over mass surveillance. Court opinions and judgements, declassified documents by the intelligence community, *amici curiae* and public interventions paint a complex picture of contestation over the enactment of non-knowledge and not just knowledge. As security and legal professionals deploy heterogeneous modes of non-knowledge to justify their practices, we need to understand how attributions of non-knowledge emerge, how they are (de)stabilised and what subjects of non-knowledge they foster. In this analysis, law and security are not set in opposition, but are understood as assemblages of knowledge and non-knowledge. Both security professionals and judges have argued from the position of non-knowledge, while NGOs and anti-surveillance activists have tended to focus on the production of knowledge. However, through reassembling non-knowledge, I have shown that novel possibilities for resistance can emerge – from the recasting of the relation between certainty and uncertainty in law to the work of reassembling of ignorance, secrecy, ambiguity and error that challenges mass surveillance.

This somewhat counterintuitive argument about the political relevance of non-knowledge has important implications for how we understand resistance to mass surveillance. Firstly, while this article has largely focused on public controversies in the US, non-knowledge has been assembled quite differently in European legal challenges. In the case of *Roman Zakharov v Russia*, the European Court of Human Rights (2015), for instance, has reiterated that 'reasonable likelihood' was sufficient in cases challenging secret surveillance. In the ongoing *Schrems v Facebook* case about data transfer to the US, the US government has asked to be a joint party, thus raising new controversies over non-knowledge (Moody 2016). Secondly, I have suggested the resisting mass surveillance entails creative and unexpected mobilisations of non-knowledge that challenge the existing work of assembling. Resistance cannot mobilise only subjects of knowledge and make claims to disclosure, transparency and making visible. It needs to work with and between the tensions and lines of assembling and reassembling. Yet, so far NGOs and anti-surveillance activists have only marginally engaged with questions of non-knowledge and have tended to mobilise them in order to produce certainty, clarity, precision, visibility and transparency. Enacting non-knowledge can have destabilising effects even beyond the public controversies I have discussed here. Finn Brunton and Helen Nissenbaum have suggested 'obfuscation' as an everyday anti-surveillance tactic through 'the production of noise modelled on the existing signal in order to make a collection of data more ambiguous, confusing, harder to exploit, more difficult to act on, and therefore less valuable' (Brunton and Nissenbaum 2015, 61). Obfuscation is effectively a device to enact uncertainty about 'leaky' data. Thirdly, assembling non-knowledge can become particularly relevant for politicising digital transformations. We need to develop fine-grained analyses of how non-knowledge is enacted through secret algorithms, the opacity of computer processes, uncertain data patterns and secret flows.

ACKNOWLEDGEMENTS

This article has benefitted from the warm engagement of audiences at Oxford Brookes University, Newcastle University, Swansea University, and University of Oxford. I am grateful to Doerthe Rosenow, Derek Bell, Angharad Closs-Stephens, Martina Tazzioli, and James Shires for the invitations to air these ideas. Many thanks to the journal editors and the anonymous reviewers for their comments and suggestions for changes.

**References**

ACLU v Clapper (2013). 13 Civ. 3994 US SDNY (27 December 2013) 2013 [cited 20 November 2014]. Available from http://www.nysd.uscourts.gov/cases/show.php?db=special&id=364.

ACLU v Clapper (2015). No 14-42 US Court of Appeals for the Second Circuit (7 May 2015) 2015 [cited 7 May 2015]. Available from http://www.ca2.uscourts.gov/decisions/isysquery/773a98db-d41d-4db8-95aa-182f994923b5/1/doc/14-42_complete_opn.pdf.

Adey, Peter, Ben Anderson, and Stephen Graham (2015) Introduction: Governing Emergencies: Beyond Exceptionality. *Theory, Culture & Society* vol. 32 (2):3-17.

Amoore, Louise (2008) Risk before Justice: When the Law Contests Its Own Suspension. *Leiden Journal of International Law* vol. 21 (4):847-861. doi: doi:10.1017/S0922156508005414.

Amoore, Louise (2011) Data Derivatives. On the emergence of a security risk calculus for our times. *Theory, Culture & Society* vol. 28 (6):24-43. doi: 10.1177/0263276411417430.

Amoore, Louise (2014) *The Politics of Possibility: Risk and security beyond probability*. Durham, NC: Duke University Press.

Amoore, Louise, and Marieke de Goede (2008) Transactions after 9/11: The banal face of the preemptive strike. *Transactions of the Institute of British Geographers* vol. 33 (2):173-185.

Anderson, Ben (2010) Security and the Future: Anticipating the Event of Terror. *Geoforum* vol. 41 (2):227-235.

Anderson Q.C., David (2016) *Report of the Bulk Powers Reviews*. Independent Reviewer of Terrorism Legislation 2016 [cited 30 August 2016]. Available from https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

Aradau, Claudia, and Tobias Blanke (2015) The (Big) Data-Security Assemblage: Knowledge and critique. *Big Data & Society* vol. 2 (2):1-12. doi: 10.1177/2053951715609066.

Aradau, Claudia, and Rens van Munster (2011) *Politics of Catastrophe: Genealogies of the unknown*. Abingdon: Routledge.

Balmer, Brian (2006) A Secret Formula, a Rogue Patent and Public Knowledge about Nerve Gas Secrecy as a Spatial–Epistemic Tool. *Social Studies of Science* vol. 36 (5):691-722.

Beck, Ulrich (2009) *World at Risk*. Cambridge: Polity.

Beck, Ulrich, and Peter Wehling (2012) The Politics of Non-Knowing: An Emerging Area of Social and Political conflict in Reflexive Modernity. In *The Politics of Knowledge*, edited by Fernando Domínguez Rubio and Patrick Baert, 33-57. London: Routledge.

Best, Jacqueline (2009) Ambiguity, Uncertainty, and Risk: Rethinking Indeterminacy. *International Political Sociology* vol. 2 (4):355-374.

Best, Jacqueline (2012) Ambiguity and Uncertainty in International Organizations: A History of Debating IMF Conditionality1. *International Studies Quarterly* vol. 56 (4):674-688.

Bigo, Didier, and Elspeth Guild (2007) Worst-Case Scenarios and the Man on the Clapham Omnibus. In *Security and Human Rights*, edited by Benjamin Goold and Liora Lazarus, 116-147. Oxford: Hart.

Breyer, Stephen (1993) *Breaking the Vicious Circle: Toward effective risk regulation*. Cambridge, Mass.: Harvard University Press.

Brunton, Finn, and Helen Nissenbaum (2015) *Obfuscation: A User's Guide for Privacy and Protest* Cambridge, MA: The MIT Press.

Bueger, Christian (2015) Making things known: epistemic practices, the United Nations, and the translation of piracy. *International Political Sociology* vol. 9 (1):1-18.

Caduff, Carlo (2015) Mind the Gap: On the Other Side of Knowing. In *Regimes of Ignorance: Anthropological Perspectives on the Production and Reproduction of Non-knowledge*, edited by Roy Dilley and Thomas G Kirsch, 31-49. New York: Bergahn Books.

Clapper, James R (2013) *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (8 June 2013) 2013 [cited 11 November 2015]. Available from http://images.politico.com/global/2013/06/08/factsonthecollectionofintelligencepursuanttosection702.html.

Clapper, James R, et al. (2014) *Brief for Defendants - Appellees* 2014, Docket No 14-42, United States Court of Appeals for the Second Circuit. Available fromhttps://www.aclu.org/legal-document/aclu-v-clapper-government-appeal-brief.

Clapper v Amnesty International USA (2013a) *Opinion of the Court*. 133 S. Ct. 1138, 1146 (2013) 2013b [cited 18 January 2015]. Available from http://www.supremecourt.gov/opinions/12pdf/11-1025_ihdj.pdf.

Clapper v Amnesty International USA (2013b) *Breyer, J., dissenting*. 568 U. S. (2013) 2013a [cited 18 January 2015]. Available from http://www.supremecourt.gov/opinions/12pdf/11-1025_ihdj.pdf.

Code, Lorraine (2014) Ignorance, Injustice and the Politics of Knowledge: Feminist Epistemology Now. *Australian Feminist Studies* vol. 29 (80):148-160.

Daase, Christopher, and Oliver Kessler (2007) Knowns and Unknowns in the War on Terror and the Political Construction of Danger. *Security Dialogue* vol. 38 (4):401-425.

de Goede, Marieke (2012) *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis: University of Minnesota Press.

de Goede, Marieke, and Beatrice de Graaf (2013) Sentencing Risk: Temporality and Precaution in Terrorism Trials. *International Political Sociology* vol. 7 (3):313-331. doi: 10.1111/ips.12025.

European Court of Human Rights (2015) *Case of Roman Zakharov v Russia*. 4 December 2015 2015 [cited 28 November 2016]. Available from http://hudoc.echr.coe.int/eng?i=001-159324.

Gros, Valentin, Marieke de Goede, and Beste İşleyen (2017) The Snowden Files Made Public: A Material Politics of Contesting Surveillance. *International Political Sociology* vol. 11 (1):73-89.

Gross, Matthias (2007) The Unknown in Process: Dynamic Connections of Ignorance, Non-Knowledge and Realted Concepts. *Current Sociology* vol. 55 (5):742-759.

Gross, Matthias (2010) *Ignorance and Surprise: Science, Society, and Ecological Design*. Cambridge, Mass.: MIT Press.

Gross, Matthias (2016) Risk as zombie category: Ulrich Beck's unfinished project of the 'non-knowledge' society. *Security Dialogue* vol. 47 (5):386-402. doi: doi:10.1177/0967010616645020.

Gross, Matthias, and Linsey McGoey (2015) Introduction. In *Routledge International Handbook of Ignorance Studies*, edited by Matthias Gross and Linsey McGoey. Abingdon: Routledge.

Hacking, Ian (1975) *The Emergence of Probability: A Philosophical Study of Early Ideas about Probability, Induction and Statistical Inference*. Cambridge: Cambridge University Press.

Home Affairs Committee (2014) Counter-Terrorism. Seventeenth Report of Session 2013–14. edited by House of Commons. London: The Stationary Office.

Jasanoff, Sheila (2011) The practices of objectivity in regulatory science. In *Social Knowledge in the Making*, edited by Charles Camic, Neil Gross and Michèle Lamont, 307-337. Chicago: University of Chicago Press.

Jewel v NSA (2013) *Order on motions for summary judgment*. US District Court for the NOrthern District of California No. C 08-04373 JSW 2013 [cited 18 November 2015]. Available from https://www.eff.org/document/order-motions-summary-judgment-0.

Jewel v NSA (2014) *Hearing Transcript Cross Motions for Summary Judgment* 2014 [cited 18 November 2015]. Available from https://www.eff.org/document/hearing-transcript-cross-motions-summary-judgment.

Jewel v NSA (2015) *Order denying plaintiffs' motion for partial summary judgment and granting defendants' motion for partial summary judgment*. No. C 08-04373 JSW 2015 [cited 30 March 2016]. Available from http://ia601302.us.archive.org/34/items/gov.uscourts.cand.207206/gov.uscourts.cand.207206.321.0.pdf.

Kessler, Oliver (2010) Risk. In *Handbook of New Security Studies*, edited by J Peter Burgess, 17-26. London: Routledge.

Kessler, Oliver (2011) The same as it never was? Uncertainty and the changing contours of international law. *Review of International Studies* vol. 37 (05):2163-2182. doi: doi:10.1017/S0260210511000386.

Krasmann, Susanne (2012) Law's knowledge: On the susceptibility and resistance of legal practices to security matters. *Theoretical Criminology* vol. 16 (4):379-394. doi: 10.1177/1362480612446775.

Ledgett, Richard H (2007) *Affidavit of Richard H. Ledgett, Jr, Acting Director, National Security Agency* (Declassifed document 28 July 2014) 2007 [cited 1 February 2016]. Available from http://www.dni.gov/files/documents/0928/Affidavit of Acting Director NSA.pdf.

Locke, John (2004 [1689]) *An Essay Concerning Humane Understanding* Volume 2 Books III and IV [Based on the Second Edition], Available from http://www.gutenberg.org/ebooks/10616.

Mills, Charles W (1997) *The Racial Contract*. Ithaca: Cornell University Press.

Mirowski, Philip (2013) *Never let a serious crisis go to waste: How neoliberalism survived the financial meltdown*. London: Verso.

Mirowski, Philip, and Edward Nik-Khah (2013) Private intellectuals and public perplexity: The economics profession and the economic crisis. *History of Political Economy* vol. 45 (suppl 1):279-311.

Moody, Glynn (2016) *US government asks to join key EU Facebook privacy case brought by Schrems* (13 June 2016). Ars Technica UK 2016 [cited 20 April 2017]. Available from https://arstechnica.co.uk/tech-policy/2016/06/eu-facebook-schrems-case-us-government-amicus-curiae/.

Neal, Andrew W (2012) Normalization and legislative exceptionalism: counterterrorist lawmaking and the changing times of security emergencies. *International Political Sociology* vol. 6 (3):260-276.

Opitz, Sven, and Ute Tellmann (2015) Future emergencies: Temporal politics in law and economy. *Theory, Culture & Society* vol. 32 (2):107-129.

Oreskes, Naomi, and Erik M Conway (2011) *Merchants of Doubt: How a handful of scientists obscured the truth on issues from tobacco smoke to global warming*. New York: Bloomsbury Press.

Oxford English Dictionary (2003) 'Non-knowledge, n.'. OED Third Edition, December 2003, Oxford University Press [cited July 03, 2017]. Available from http://www.oed.com/view/Entry/127989?redirectedFrom=nonknowledge.

Pinto, Manuela Fernández (2015) Tensions in agnotology: Normativity in the studies of commercially driven ignorance. *Social Studies of Science* vol. 45 (2):294-315. doi: 10.1177/0306312714565491.

Privacy and Civil Liberties Oversight Board (2014) *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 2014 [cited 10 December 2015]. Available from https://www.pclob.gov/library/702-Report.pdf.

Proctor, Robert N (2011) *Golden Holocaust: Origins of the Cigarette Catastrophe and the Case for Abolition*. Berkeley, CA: University of California Press.

Proctor, Robert N (2008) A missing term to describe the cultural production of ignorance (and its study). In *Agnotology: The Making & Unmaking of Ignorance*, edited by Robert N Proctor and Londa Schiebinger, 1-36. Stanford, CA: Stanford University Press.

Rabinow, Paul (2003) *Anthropos Today. Reflections on Modern Equipment*. Princeton: Princeton University Press.

Rancière, Jacques (1991) *The Ignorant Schoomaster. Five Lessons in Intellectual Emancipation*. Translated by Kristin Ross. Stanford, California: Stanford University Press.

Rasmussen, Mikkel Vedby (2006) *The Risk Society at War. Terror, Technology and Strategy in the Twenty-First Century*. Cambridge: Cambridge University Press.

Scheuerman, William E (1994) *Between the Norm and the Exception. The Frankfurt School and the rule of law*. Massachusetts: MIT Press.

Scheuerman, William E (2006) Survey Article: Emergency Powers and the Rule of Law After 9/11*. *Journal of Political Philosophy* vol. 14 (1):61-84.

Shapiro, Barbara J (1983) *Probability and Certainty in Seventeenth-Century England. A study of the relationships between natural science, religion, history, law, and literature*. Princeton, NJ: Princeton University Press.

Smithson, Michael (2008) Social theories of ignorance. In *Agnotology: The Making and Unmaking of Ignorance*, edited by Robert Proctor and Londa Schiebinger, 209-229. Stanford, CA: Stanford University Press.

Tuana, Nancy (2004) Coming to Understand: Orgasm and the Epistemology of Ignorance. *Hypatia* vol. 19 (1):194-232.

Valverde, Mariana (2003) *Law's Dream of a Common Knowledge*. Edited by Austin Sarat, *The Cultural Lives of Law*. Princeton: Princeton University Press.

Vermeir, Koen, and Daniel Margocsy (2012) States of Secrecy: An Introduction. *The British Journal for the History of Science* vol. 45 (2):153-164. doi: 10.1017/S0007087412000052.

Walters, William, and Alex Luscombe (2017) Hannah Arendt and the Art of Secrecy; Or, the Fog of Cobra Mist1. *International Political Sociology* vol. 11 (1):5-20. doi: 10.1093/ips/olw027.

Whatmore, Sarah J (2009) Mapping knowledge controversies: science, democracy and the redistribution of expertise. *Progress in Human Geography* vol. 33 (5):587-598. doi: doi:10.1177/0309132509339841.

Wikimedia et al v NSA (2015a) *Memorandum in support of the Government's motion to dismiss*. 08 August 2015 2015a [cited 28 November 2016]. Available from https://www.aclu.org/legal-document/wikimedia-v-nsa-defendants-motion-dismiss-first-amended-complaint.

Wikimedia et al v NSA (2015b) *Memorandum Opinion*. No. 15-cv-662 US District Court of Maryland (23 October 2015) 2015b [cited 15 January 2016]. Available from https://www.aclu.org/legal-document/wikimedia-v-nsa-d-md-opinion.

Wikimedia et al v NSA (2016) *Brief for Plaintiffs-Appelants*. No. 15-2560 2016 [cited 30 March 2017]. Available from https://www.aclu.org/legal-document/wikimedia-v-nsa-aclu-4th-cir-appeal-brief.